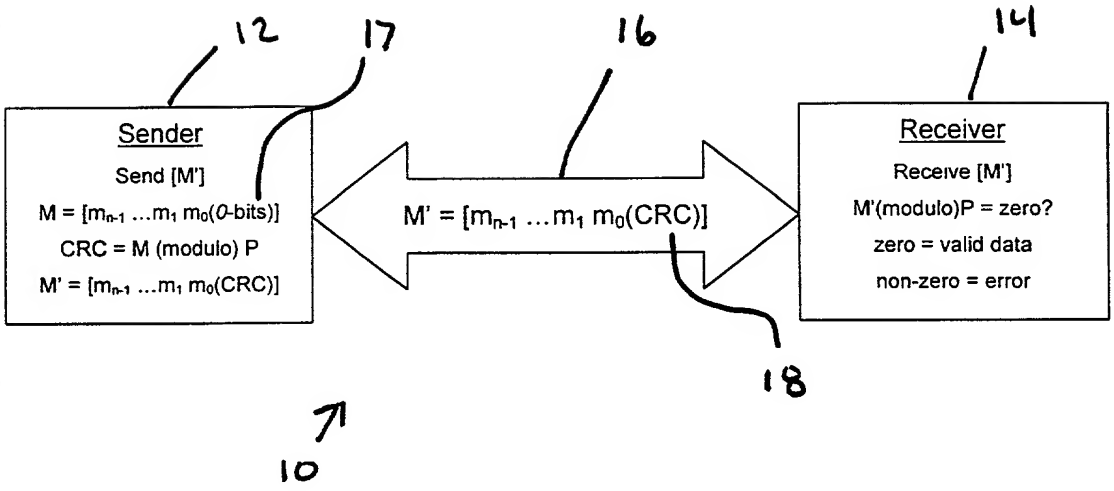

FIG. 1
(prior art)

Docket # 10559-576001 Application # 09/755,605

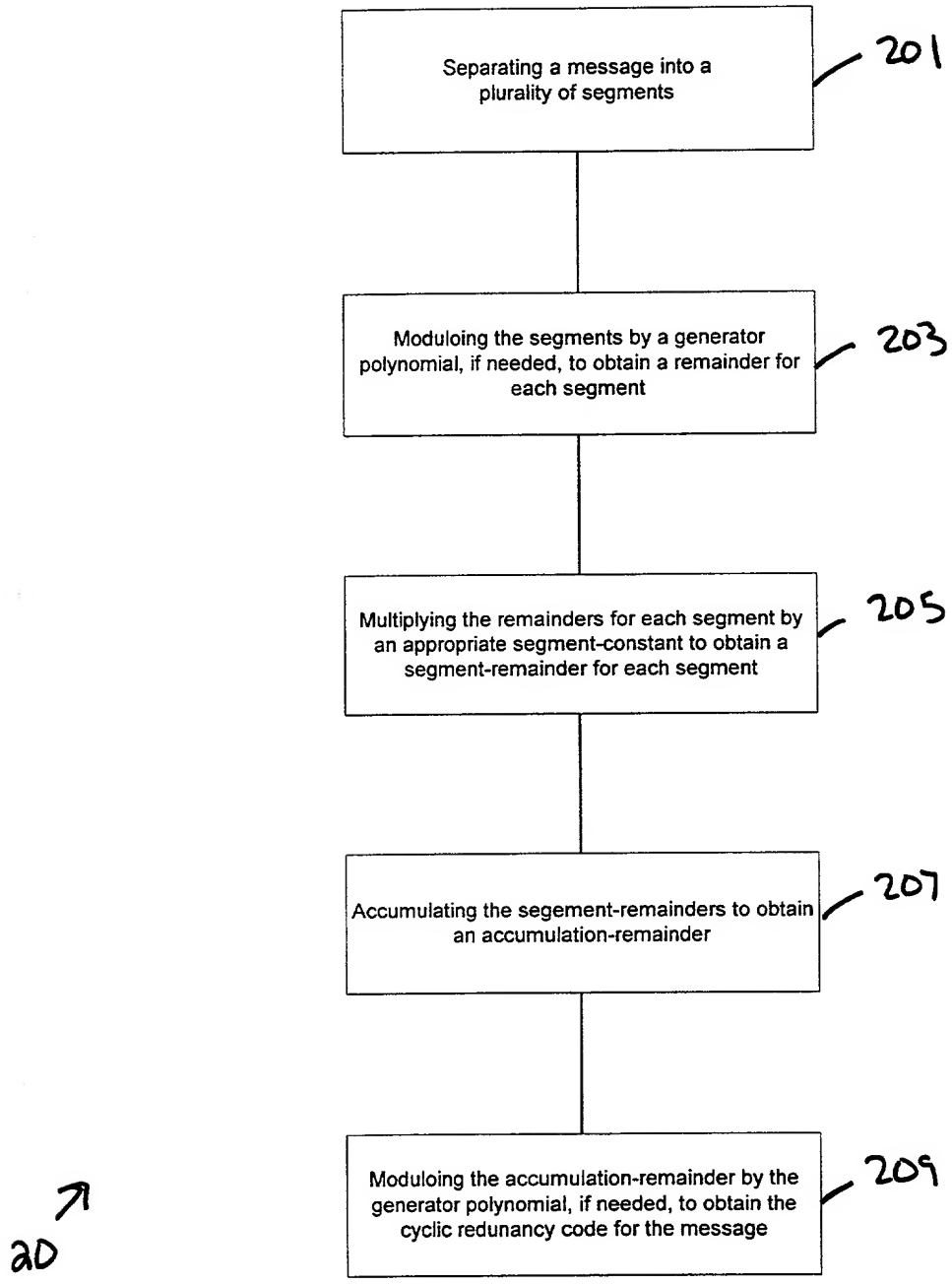
Separating a message into a plurality of segments
201
Moduloing the segments by a generator polynomial, if needed, to obtain a remainder for each segment
203
Multiplying the remainders for each segment by an appropriate segment-constant to obtain a segment-remainder for each segment
205
Accumulating the segement-remainders to obtain an accumulation-remainder
207
Moduloing the accumulation-remainder by the generator polynomial, if needed, to obtain the cyclic redunancy code for the message
209
20

FIG. 2

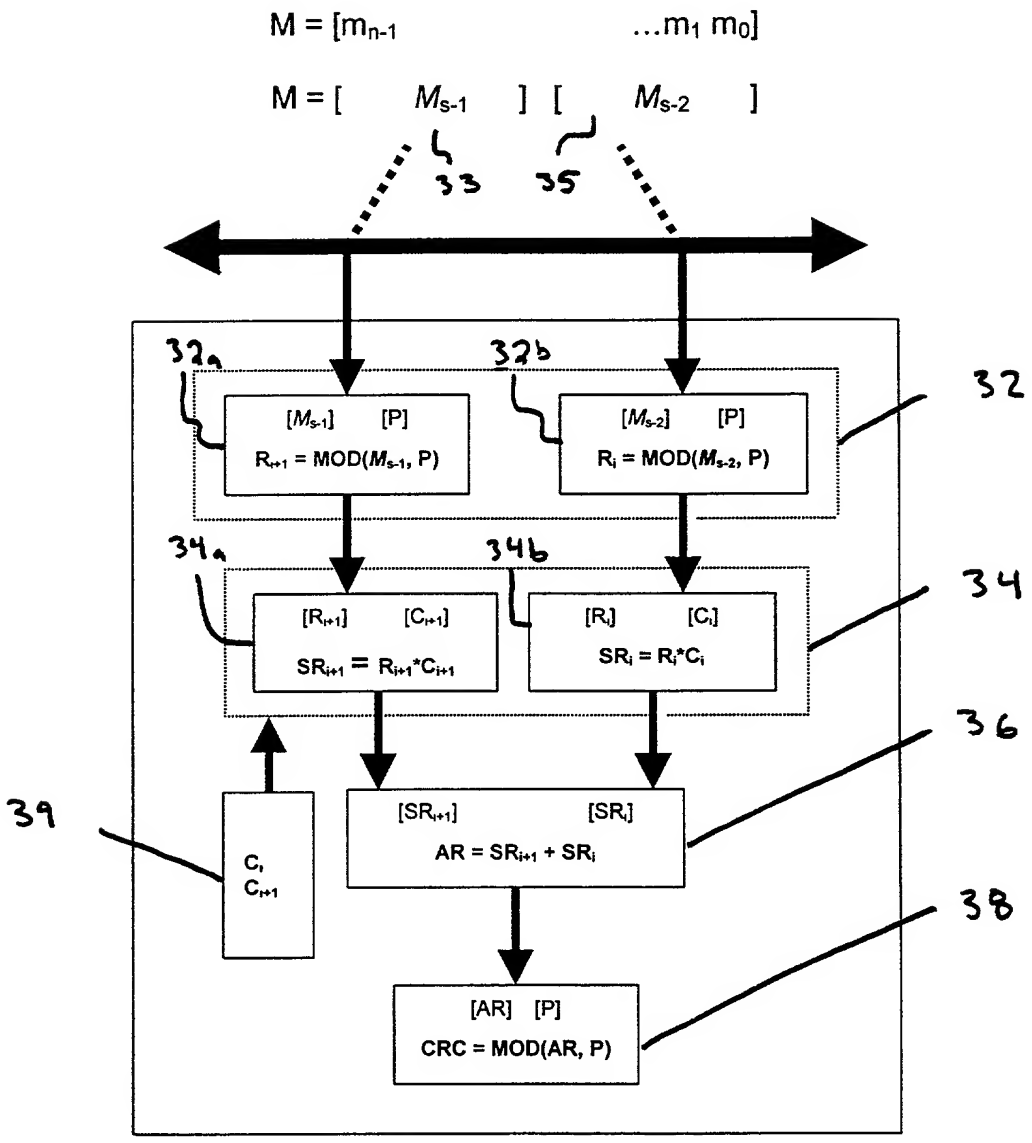
M = [m_{n-1} ...m_1 m_0]
M = [M_{s-1}] [M_{s-2}]
33
35
32a
32b
32
[M_{s-1}] [P]
R_{i+1} = MOD(M_{s-1}, P)
[M_{s-2}] [P]
R_i = MOD(M_{s-2}, P)
34a
34b
34
[R_{i+1}] [C_{i+1}]
SR_{i+1} = R_{i+1}*C_{i+1}
[R_i] [C_i]
SR_i = R_i*C_i
36
39
C_i
C_{i+1}
[SR_{i+1}] [SR_i]
AR = SR_{i+1} + SR_i
38
[AR] [P]
CRC = MOD(AR, P)
30

FIG. 3

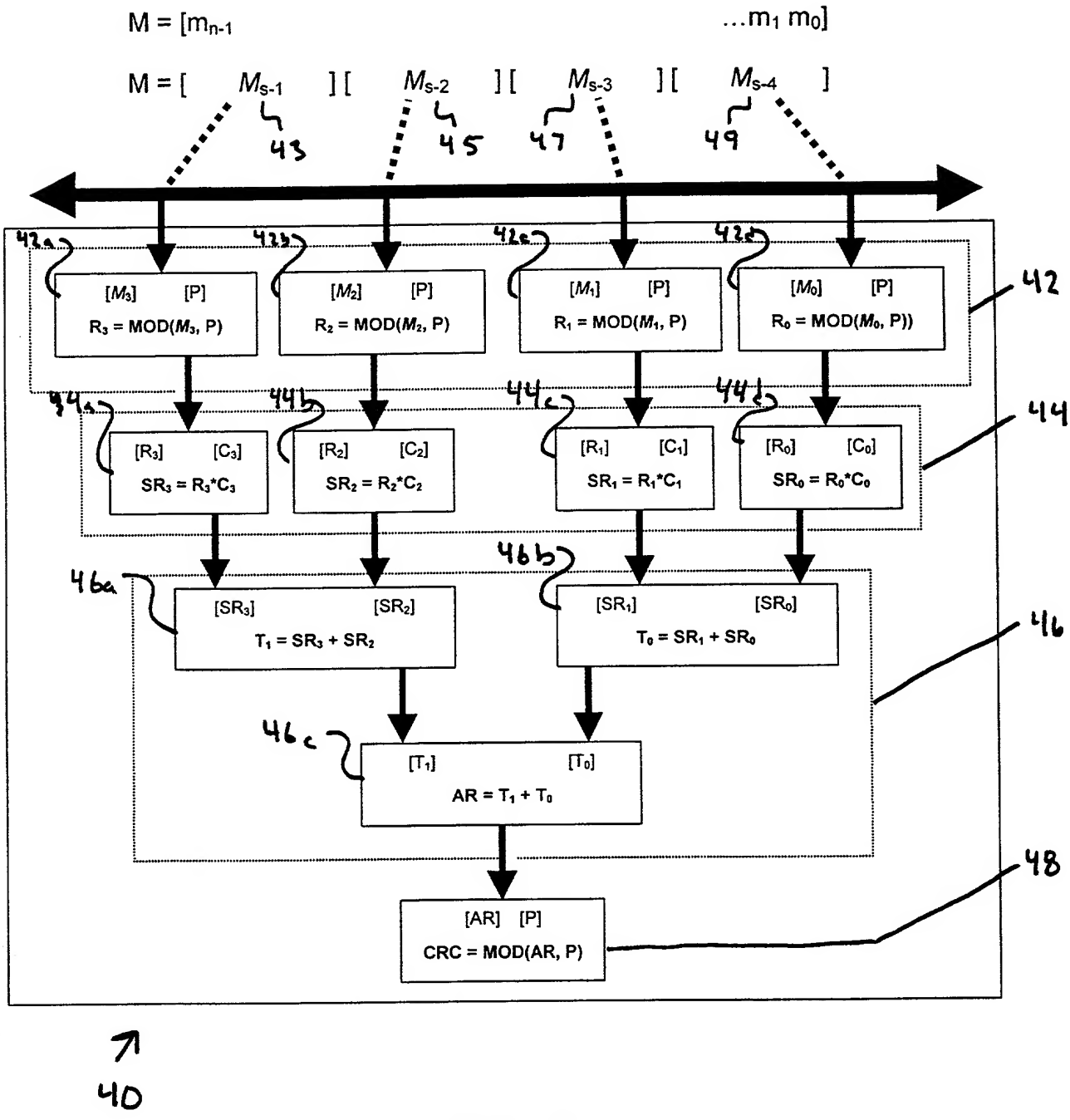
M = [m_{n-1} ... m_1 m_0]
M = [M_{S-1}][M_{S-2}][M_{S-3}][M_{S-4}]
43
45
47
49
42a
42b
42c
42d
[M3] [P]
R3 = MOD(M3, P)
[M2] [P]
R2 = MOD(M2, P)
[M1] [P]
R1 = MOD(M1, P)
[M0] [P]
R0 = MOD(M0, P))
42
44a
44b
44c
44d
[R3] [C3]
SR3 = R3*C3
[R2] [C2]
SR2 = R2*C2
[R1] [C1]
SR1 = R1*C1
[R0] [C0]
SR0 = R0*C0
44
46a
46b
[SR3] [SR2]
T1 = SR3 + SR2
[SR1] [SR0]
T0 = SR1 + SR0
46
46c
[T1] [T0]
AR = T1 + T0
[AR] [P]
CRC = MOD(AR, P)
48
40

FIG. 4

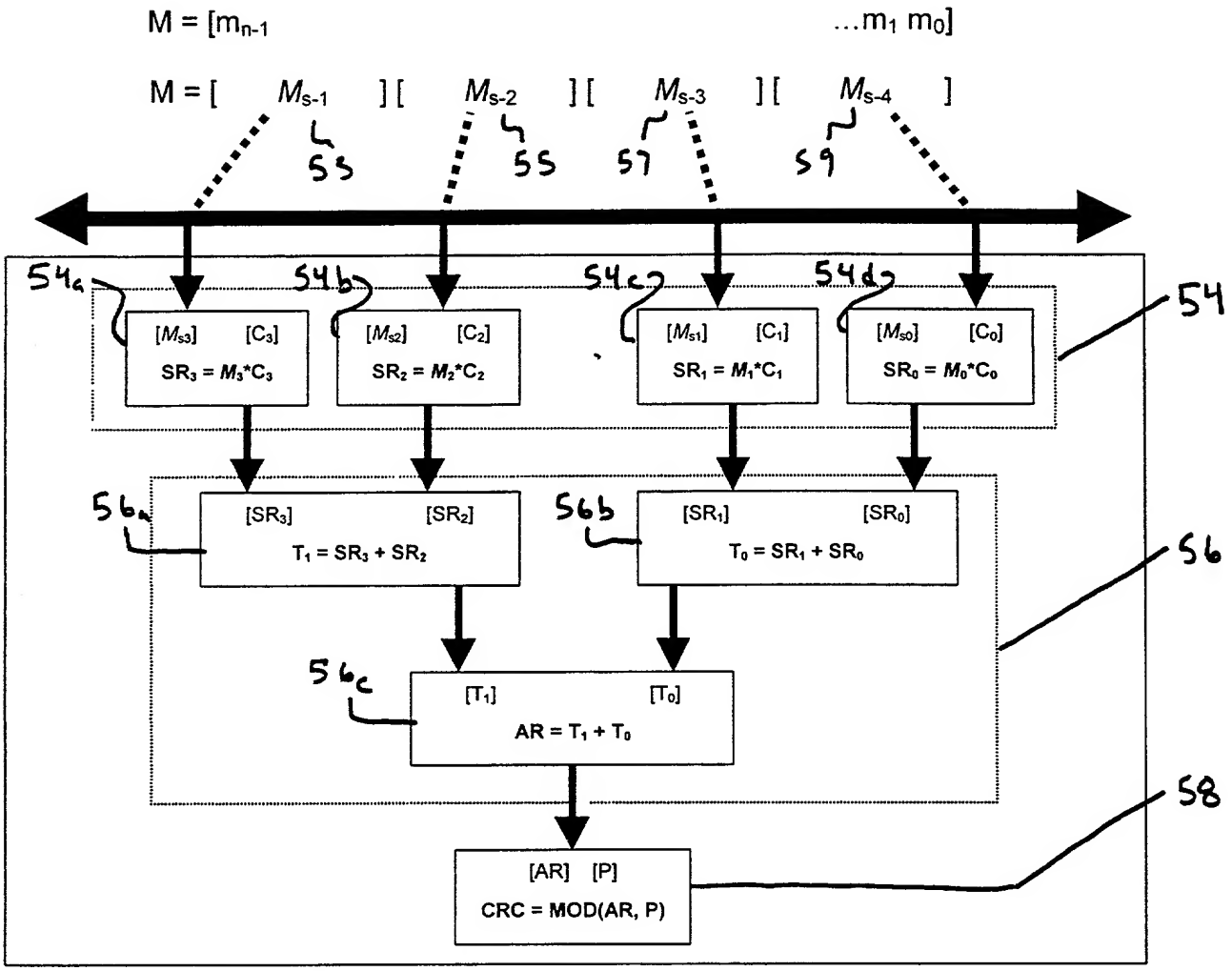
M = [m n-1 ...m 1 m 0]
M = [Ms-1][Ms-2][Ms-3][Ms-4]
55
55
57
59
54a
54b
54c
54d
54
[Ms3] [C3]
SR3 = M3*C3
[Ms2] [C2]
SR2 = M2*C2
[Ms1] [C1]
SR1 = M1*C1
[Ms0] [C0]
SR0 = M0*C0
56a
56b
56
[SR3] [SR2]
T1 = SR3 + SR2
[SR1] [SR0]
T0 = SR1 + SR0
56c
[T1] [T0]
AR = T1 + T0
58
[AR] [P]
CRC = MOD(AR, P)

FIG. 5

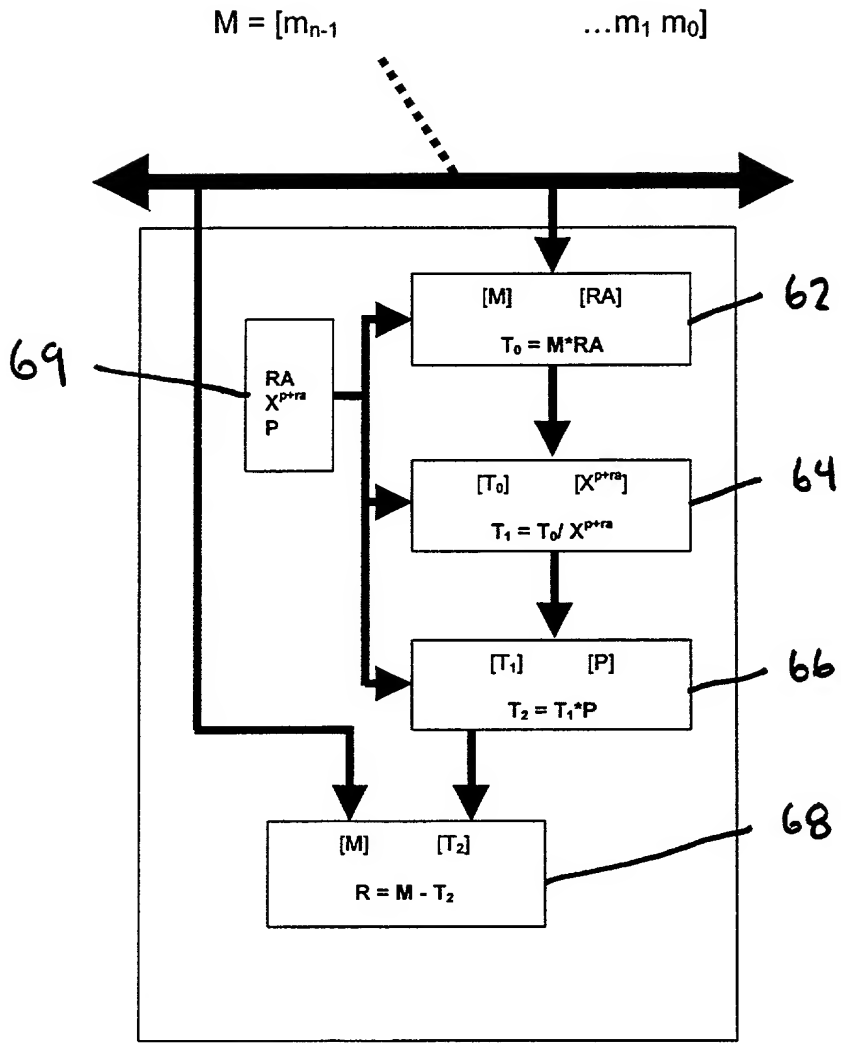
M = [m$_{n-1}$ ...m$_1$ m$_0$]
[M] [RA]
T$_0$ = M*RA
62
69
RA
X^{p+ra}
P
[T$_0$] [X^{p+ra}]
T$_1$ = T$_0$/ X^{p+ra}
64
[T$_1$] [P]
T$_2$ = T$_1$*P
66
[M] [T$_2$]
R = M - T$_2$
68

FIG. 6

60

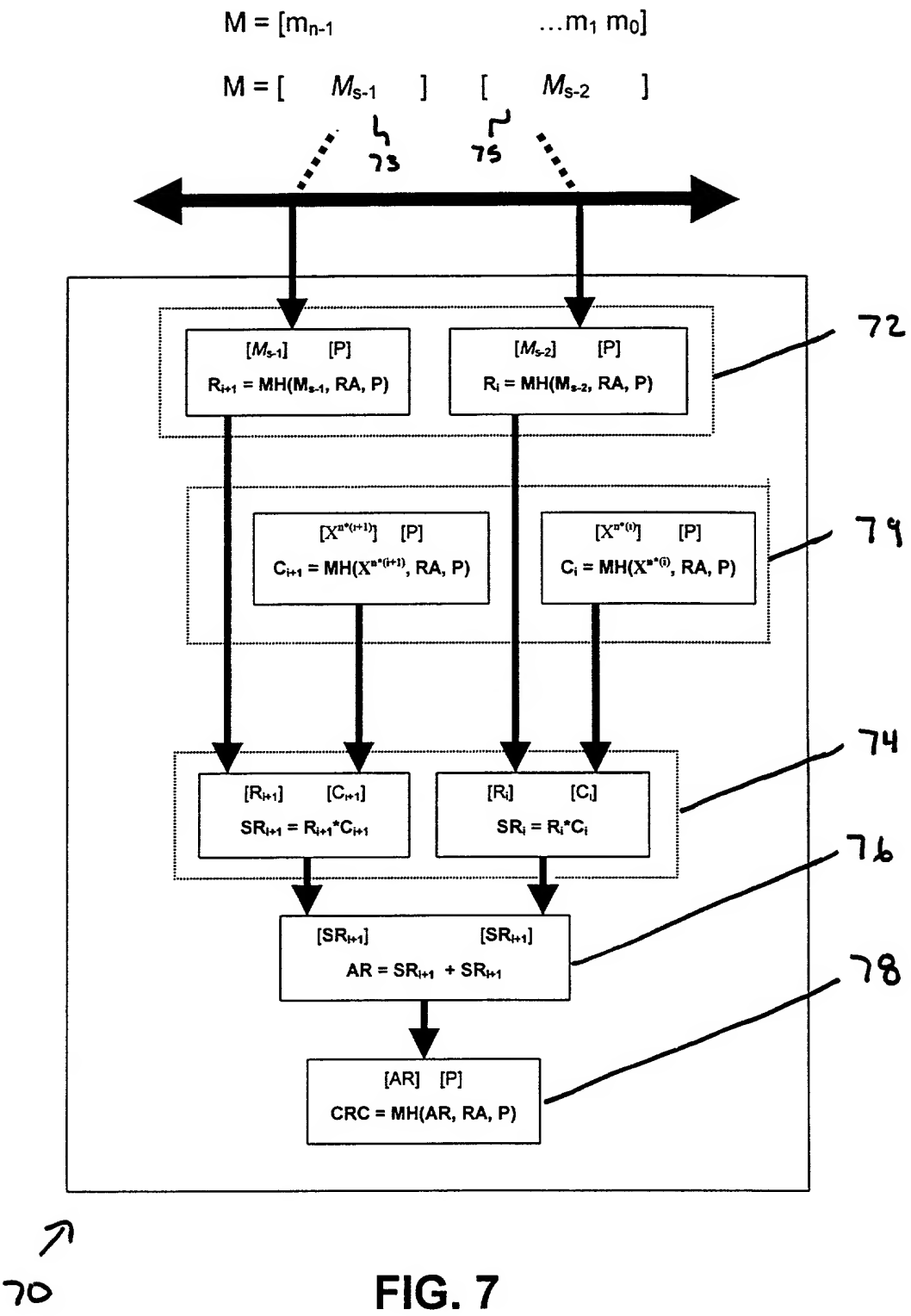
M = [m_{n-1} ...m_1 m_0]
M = [M_{s-1}] [M_{s-2}]
73
75
[M_{s-1}] [P]
R_{i+1} = MH(M_{s-1}, RA, P)
[M_{s-2}] [P]
R_i = MH(M_{s-2}, RA, P)
72
[X^{n*(i+1)}] [P]
C_{i+1} = MH(X^{n*(i+1)}, RA, P)
[X^{n*(i)}] [P]
C_i = MH(X^{n*(i)}, RA, P)
79
[R_{i+1}] [C_{i+1}]
SR_{i+1} = R_{i+1}*C_{i+1}
[R_i] [C_i]
SR_i = R_i*C_i
74
[SR_{i+1}] [SR_{i+1}]
AR = SR_{i+1} + SR_{i+1}
76
[AR] [P]
CRC = MH(AR, RA, P)
78
70

FIG. 7

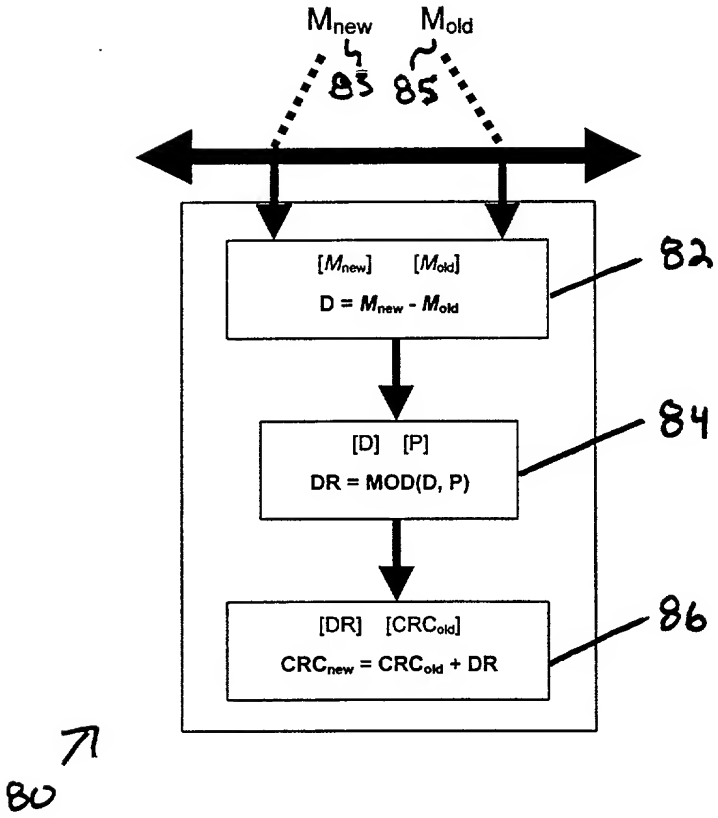
Mnew
Mold
83
85
[Mnew] [Mold]
D = Mnew - Mold
82
[D] [P]
DR = MOD(D, P)
84
[DR] [CRCold]
CRCnew = CRCold + DR
86
80

FIG. 8

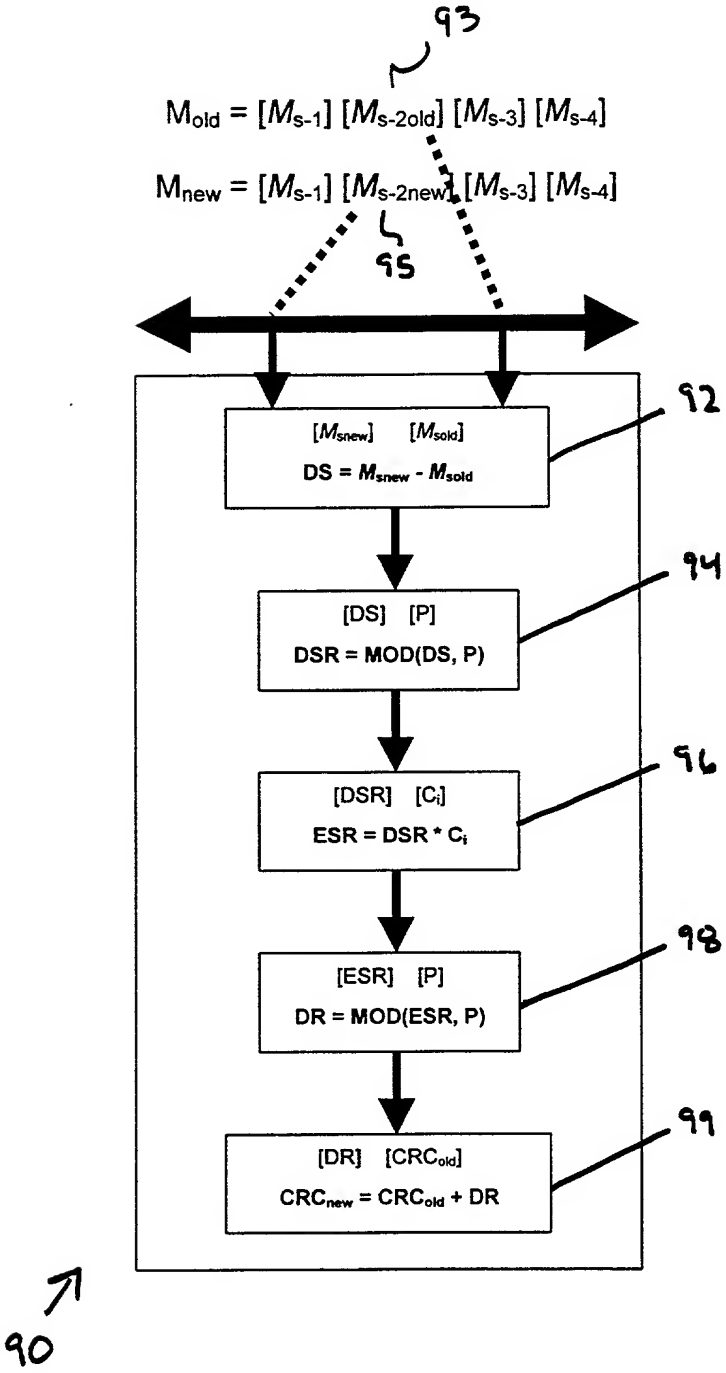
93
$M_{old} = [M_{s-1}] [M_{s-2old}] [M_{s-3}] [M_{s-4}]$
$M_{new} = [M_{s-1}] [M_{s-2new}] [M_{s-3}] [M_{s-4}]$
95
92
$[M_{snew}]$ $[M_{sold}]$
$DS = M_{snew} - M_{sold}$
94
[DS] [P]
DSR = MOD(DS, P)
96
[DSR] $[C_i]$
$ESR = DSR * C_i$
98
[ESR] [P]
DR = MOD(ESR, P)
99
[DR] $[CRC_{old}]$
$CRC_{new} = CRC_{old} + DR$
90

FIG. 9

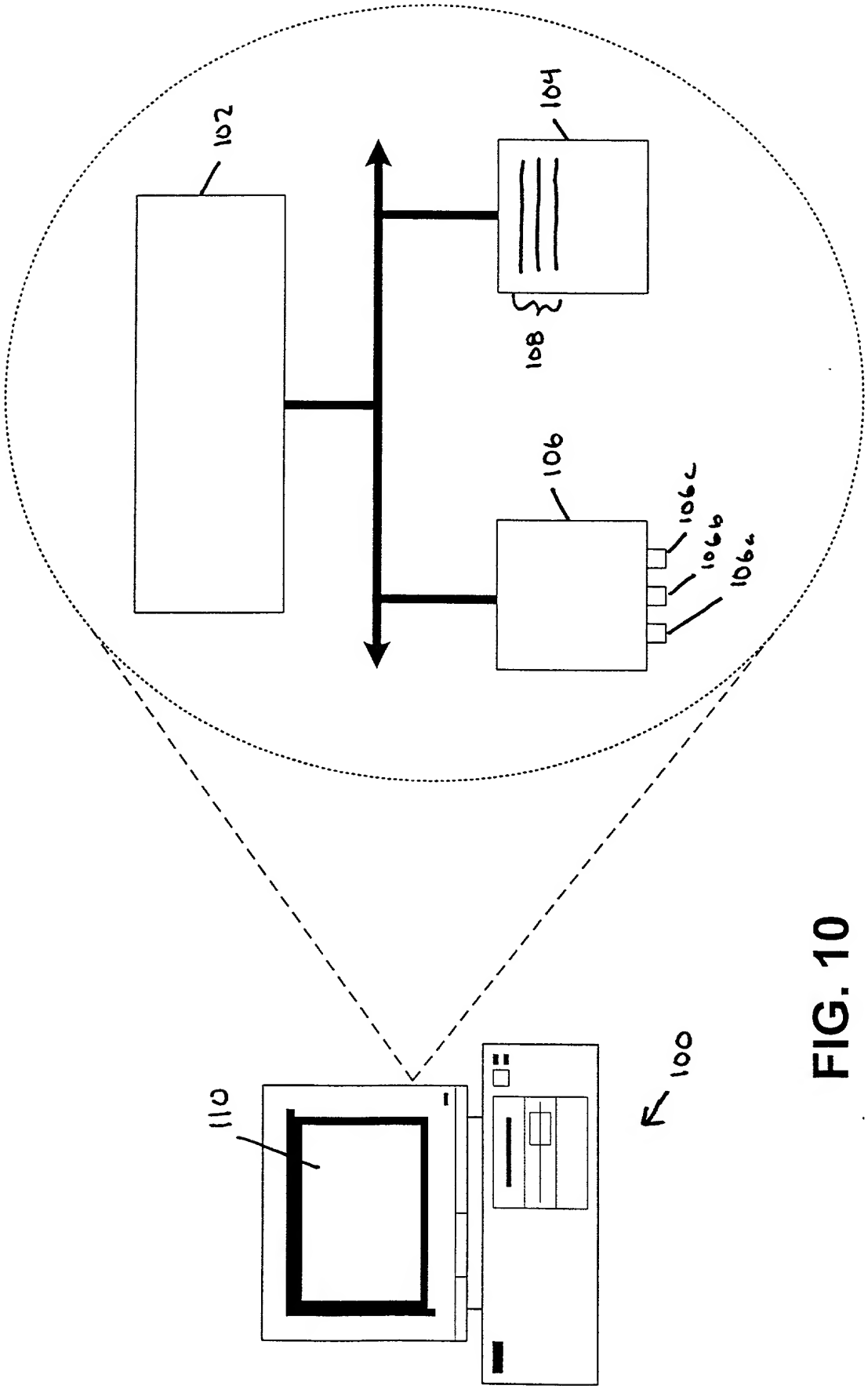

FIG. 10

20070250-576001